UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/820,682	04/08/2004	Ziv Haparnas	1005-11-01 USP	8531

42698 7590 01/29/2008

FARSHAD JASON FARHADIAN
CENTURY IP LAW GROUP
P.O. BOX 7333
NEWPORT BEACH, CA 92658-7333

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
01/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/820,682	HAPARNAS, ZIV	
	Examiner	Art Unit	
	Oscar A. Louie	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 November 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-6,8,10 and 11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-6,8,10 and 11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/ are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This final action is in response to the amendment filed on 11/15/2007. Claims 1, 2, 4-6, 8, 10, & 11 are pending and have been considered as follows.

Claim Objections

1. Claims 1 & 11 are objected to because of the following informalities:

   - Claim 1 line 1 recites the term "for" which should be "... of..."
   - Claim 11 lines 1, 4, 8, 10, 12, & 14 recite the term "for" which should be "... configured to..."

   Appropriate correction is required.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 2, 4-6, 8, 10, & 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ketcham (US-6075860-A) in view of Chan et al. (US-5970144-A) and in further view of Kaliski, Jr. (US-6085320-A).

Claim 1:

Ketcham discloses a secured communication method for a mobile communications network comprising,

- "receiving a request to provide a security key to a mobile device connected to the mobile communications network" (i.e. "Account generator 200 comprises a key generator 202 receptive to an authorization request for generation of a cryptographically suitable authentication encryption key") [column 6 lines 48-51];
- "generating a unique security key for the requesting mobile device using a public or private key mechanism unless the unique security key is preprogrammed into the mobile device" (i.e. "Key generator 202 generates authentication encryption key") [column 6 lines 51-52];
- "forwarding the unique security key to the mobile device" (i.e. "FIG. 2 is a functional block diagram depicting the generation, distribution, and processing of authentication keys in accordance with one embodiment of the present invention") [column 6 lines 42-45];

but, does not disclose,

- "storing the unique security key in a first data structure mechanism in association with a unique value identifying the mobile device," although Chan et al. do suggest that both the service provider and mobile station store authentication information, as recited below;
- "storing the unique security key in a second data structure mechanism in the mobile device," although Chan et al. do suggest that both the service provider and mobile station store authentication information, as recited below;

- "receiving a request to provide the unique security key for the mobile device to a service provider," although Kaliski, Jr. does suggest receiving a request to provide authentication information for a client to a server, as recited below;
- "approving the request to provide the unique security key based on content of a list of approved service providers, if a first condition is met," although Kaliski, Jr. does suggest the usage of a control list, as recited below;
- "wherein the first condition is set by the mobile device," although Kaliski, Jr. does suggest a condition of time to determine approval, as recited below;
- "providing the unique security key to the service provider, if the service provider is approved to receive the unique security key for the mobile device," although Kaliski, Jr. does suggest sending authentication information to a server once approved, as recited below;

however, Chan et al. do disclose,

- "only the MS 102 and the SAMS 204 store the sensitive authentication information in the preferred embodiment of the present invention" [column 5 lines 51-52];

whereas, Kaliski, Jr. does disclose,

- "Client 20 receives the message 11 sent over the communications channel 15, verifies the signature on the certificate with the trusted certification authority's public key 24 in public key operation 32 and verification process 33, and processes the certificate in operation 30 to read and store the public key of the server" [column 8 lines 26-31];

- "Reference to the list during the initial stages of the protocol will indicate whether the transaction being initiated is with a valid server or with one holding a revoked certificate, and thereby whether a received server's certificate is to be verified" [column 4 lines 5-9];
- "Once client 20 verifies the time-varying value from 42 and the certificate 41 of server 40, trust of the server 40 is established" [column 8 lines 49-51];
- "The encrypted message 12, [KSS.vertline.TS]PUB.sub.SERV, is sent to the server 40 where it is received and processed for recovery" [column 8 lines 61-62];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "storing the unique security key in a first data structure mechanism in association with a unique value identifying the mobile device" and "storing the unique security key in a second data structure mechanism in the mobile device" and "receiving a request to provide the unique security key for the mobile device to a service provider" and "approving the request to provide the unique security key based on content of a list of approved service providers, if a first condition is met" and "wherein the first condition is set by the mobile device" and "providing the unique security key to the service provider, if the service provider is approved to receive the unique security key for the mobile device," in the invention as disclosed by Ketcham since it would be reasonable to expect one of ordinary skill in the art at the time of the applicant's invention to store authentication information as suggested by Ketcham, Chan et al., and Kaliski, Jr. The inclusion of Kaliski, Jr. would have been obvious to one of ordinary skill in the art at the time of the applicant's invention since it is typical to use a central authority when implementing a variant of PKI for the purposes of authenticating and verifying both the client(s) and the server(s).

Claim 2:

Ketcham, Chan et al., and Kaliski, Jr. disclose a secured communication method for a mobile communications network, as in Claim 1 above, but the combination of Ketcham and Chan et al. do not disclose,

- "denying the request to provide the unique security key, if the service provider is not approved to receive the unique security key for the mobile device," although Kaliski, Jr. does suggest terminating a transaction upon failure to verify, as recited below;

however, Kaliski, Jr. does disclose,

- "A failure to verify the server's certificate or validate the received time-varying value terminates the transaction" [column 8 lines 37-39];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "denying the request to provide the unique security key, if the service provider is not approved to receive the unique security key for the mobile device," in the invention as disclosed by Ketcham and Chan et al. for the purposes of denying access upon verification failure.

Claims 4-6 & 8:

Ketcham, Chan et al., and Kaliski, Jr. disclose a secured communication method for a mobile communications network, as in Claim 1 above, their combination further disclosing,

- "the second data storage mechanism is a memory chip" (i.e. "Authentication card 118 is a portable storage device such as a smart card that may be conveniently transported by an authorized user to a remote terminal") [column 8 lines 19-21];

- "the second data storage mechanism is an identity module for the mobile device" (i.e. "Authentication card 118 stores an MSID 204, an authentication encryption key 206, and optionally may store other information such as algorithmic identifiers 402, optional parameters 412 for configuring or personalizing a remote terminal 102 according to an authorized user's preferences") [column 8 lines 13-18];
- "the second data storage mechanism is a SIM card for the mobile device" (i.e. "authentication card 118 takes the form of a GSM subscriber identity module (SIM)") [column 8 lines 21-23];
- "the unique value is at least one of the mobile device's electronic serial number (ESN), international mobile equipment identity (IMEI) and phone number" (i.e. "Authentication card 118 stores an MSID 204, an authentication encryption key 206, and optionally may store other information such as algorithmic identifiers 402, optional parameters 412 for configuring or personalizing a remote terminal 102 according to an authorized user's preferences") [column 8 lines 13-18].

Claim 10:

Ketcham, Chan et al., and Kaliski, Jr. disclose a secured communication method for a mobile communications network, as in Claim 1 above, but the combination of Ketcham and Chan et al. do not disclose,

- "the list of approved service providers is stored in the mobile device," although Kaliski, Jr. does suggest a client control list, as recited below;

however, Kaliski, Jr. does disclose,

- "The client CRL would serve, for example, as a list of revoked smart cards, i.e., cards that have been lost, stolen, destroyed or that have expired" [column 7 lines 50-52];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the list of approved service providers is stored in the mobile device," in the invention as disclosed by Ketcham and Chan et al. for the purposes of verifying proper servers.

Claim 11:

Ketcham discloses a security system for managing security key assignment in a mobile communications network comprising,

- "a key generating mechanism for generating a unique security key for a mobile device, using a public or private key mechanism unless the unique security key is preprogrammed into the mobile device, in response to a request received by the security system from the mobile device" (i.e. "Both carrier 140 and activating wireless communication device 110 generate the same A-Key (or encryption key) independently and perform mutual authentication") [column 6 lines 42-45];
- "a transmission mechanism for transmitting the unique security key to the mobile device" (i.e. "Both carrier 140 and activating wireless communication device 110 generate the same A-Key (or encryption key) independently and perform mutual authentication") [column 6 lines 42-45];

but, does not disclose,

- "a first data storage mechanism for storing the unique security key for the mobile device in association with an identifier identifying the mobile device," although Chan et al. do suggest that both the service provider and mobile station store authentication information, as recited below;
- "a second data storage mechanism for storing the unique security key in the mobile device," although Chan et al. do suggest that both the service provider and mobile station store authentication information, as recited below;
- "a verification mechanism for verifying whether a service provider is an approved service provider before the unique security key is transmitted to the service provider based on content of a list of approved service providers, if a first condition is met," although Kaliski, Jr. does suggest a verification unit, as recited below;
- "wherein the first condition is set by the mobile device and communicated to the security system," although Kaliski, Jr. does suggest a condition of time to determine approval, as recited below;
- "wherein the unique security key is transmitted to the service provider, in response to a request submitted by the service provider to the security system," although Kaliski, Jr. does suggest sending authentication information to a server once approved, as recited below;

however, Chan et al. do disclose,

- "only the MS 102 and the SAMS 204 store the sensitive authentication information in the preferred embodiment of the present invention" [column 5 lines 51-52];

whereas, Kaliski, Jr. does disclose,

- "Checking of the time-varying value to see that it is valid is done in comparison unit 34" [column 8 lines 36-37];
- "Once client 20 verifies the time-varying value from 42 and the certificate 41 of server 40, trust of the server 40 is established" [column 8 lines 49-51];
- "The encrypted message 12, [KSS.vertline.TS]PUB.sub.SERV, is sent to the server 40 where it is received and processed for recovery" [column 8 lines 61-62];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a first data storage mechanism for storing the unique security key for the mobile device in association with an identifier identifying the mobile device" and "a second data storage mechanism for storing the unique security key in the mobile device" and "a verification mechanism for verifying whether a service provider is an approved service provider before the unique security key is transmitted to the service provider based on content of a list of approved service providers, if a first condition is met" and "wherein the first condition is set by the mobile device and communicated to the security system" and "wherein the unique security key is transmitted to the service provider, in response to a request submitted by the service provider to the security system," in the invention as disclosed by Ketcham since it would be reasonable to expect one of ordinary skill in the art at the time of the applicant's invention to store authentication information as suggested by Ketcham, Chan et al., and Kaliski, Jr. The

inclusion of Kaliski, Jr. would have been obvious to one of ordinary skill in the art at the time of the applicant's invention since it is typical to use a central authority when implementing a variant of PKI for the purposes of authenticating and verifying both the client(s) and the server(s).

Response to Arguments

4. Applicant's arguments filed 11/15/2007 have been fully considered but they are not persuasive.

Regarding Arguments Pertaining to Ketcham:

- The applicant's argument that state, "Ketcham fails to disclose "receiving a request to provide the unique security key for the mobile device to a service provider," has been considered but is non-persuasive. Ketcham discloses, "Account generator 200 comprises a key generator 202 receptive to an authorization request for generation of a cryptographically suitable authentication encryption key" [column 6 lines 48-51].

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
01/23/2007

Nasser Moazzami
Supervisory Patent Examiner

1/23/08